EXHIBIT F

US 20160110819A1

(19) United States
(12) Patent Application Publication
Abramowitz
(10) Pub. No.: US 2016/0110819 A1
(43) Pub. Date: Apr. 21, 2016

(54) **DYNAMIC SECURITY RATING FOR CYBER INSURANCE PRODUCTS**

(71) Applicant: **Marc Lauren Abramowitz**, Palo Alto, CA (US)

(72) Inventor: **Marc Lauren Abramowitz**, Palo Alto, CA (US)

(21) Appl. No.: **14/918,398**

(22) Filed: **Oct. 20, 2015**

Related U.S. Application Data

(60) Provisional application No. 62/066,716, filed on Oct. 21, 2014.

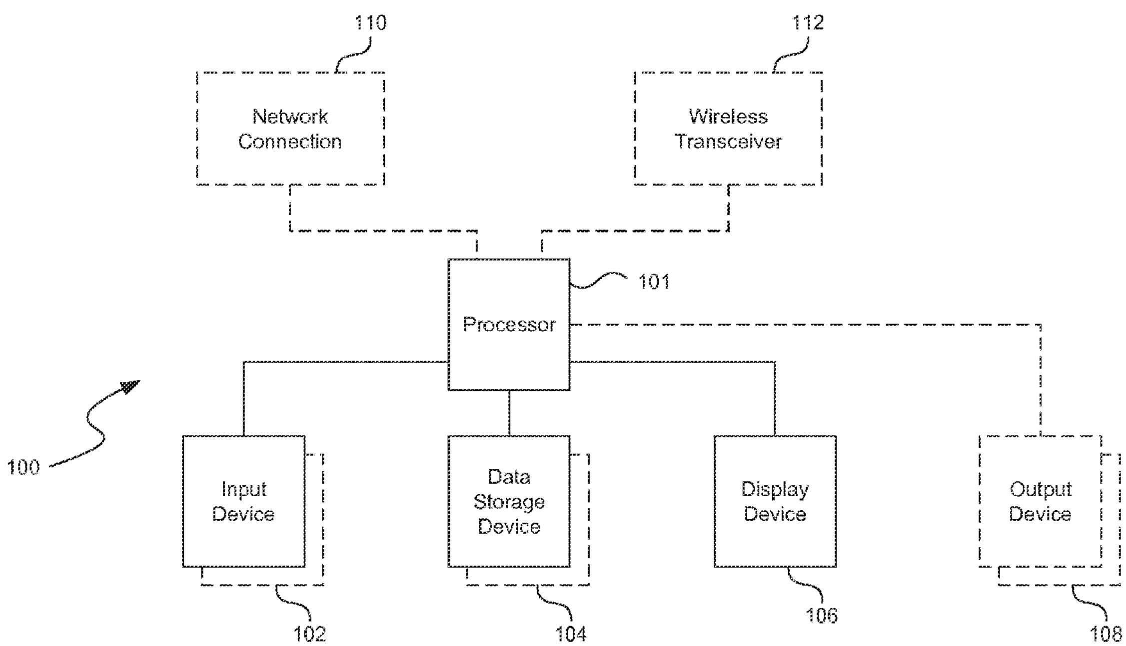
Publication Classification

(51) **Int. Cl.**
G06Q 40/08 (2006.01)
H04L 29/06 (2006.01)

(52) **U.S. Cl.**
CPC ***G06Q 40/08*** (2013.01); ***H04L 63/1433*** (2013.01); ***H04L 63/1425*** (2013.01)

(57) **ABSTRACT**

In one or more embodiments, the technology determines one or more cyber insurance policies and/or products based on a company's real-time exposure to a cyber attack on one or more of its computing asset's. The technology performs various security analysis techniques to explore, locate, and evaluate a company's network/assets for creating risk and damage assessments that are used for dynamically determining a cyber insurance that is tailored to that company at that moment of time and, optionally, based on future projections. The technology can continuously or semi-continuously monitor the company's network for any changes and, upon detection of changes that could affect the company's exposure to a cyber attack, provides information associated with the detected changes as feedback to allow determination of new/modified cyber insurance policies/products.



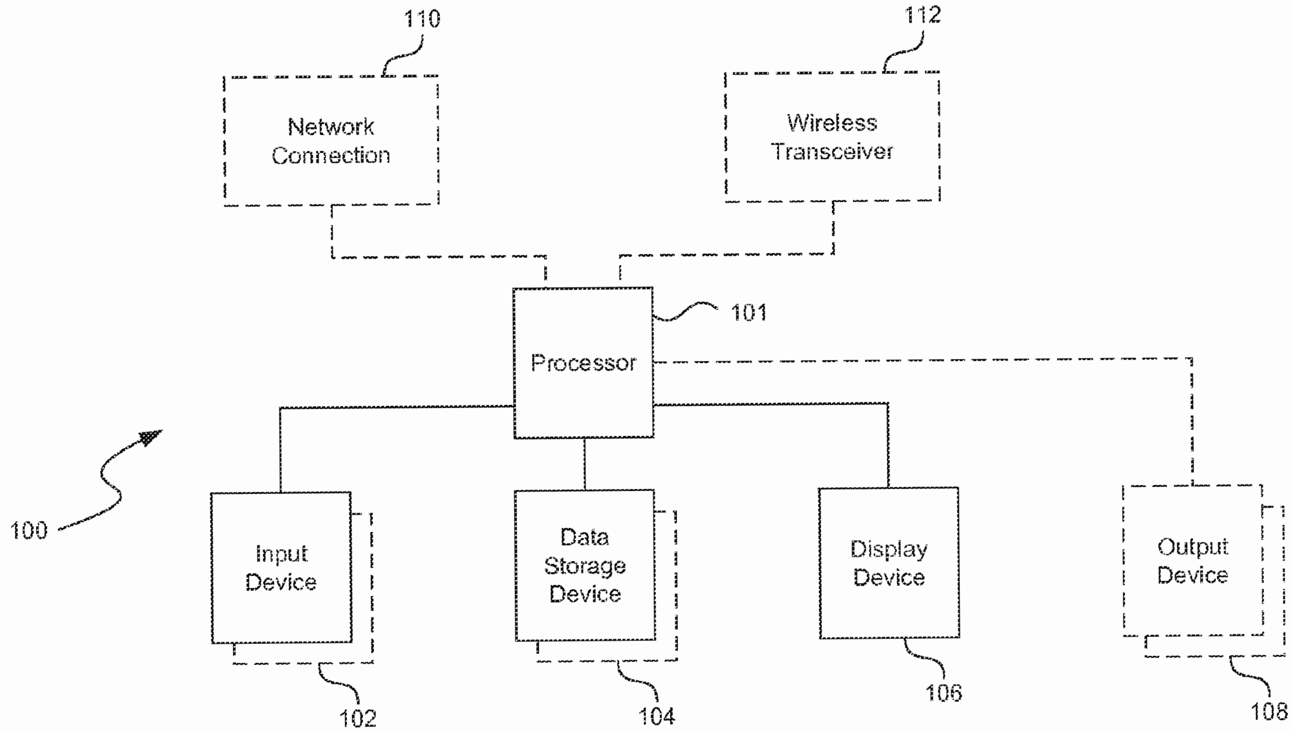

110
Network Connection
112
Wireless Transceiver
Processor
101
100
Input Device
Data Storage Device
Display Device
Output Device
102
104
106
108

FIG. 1

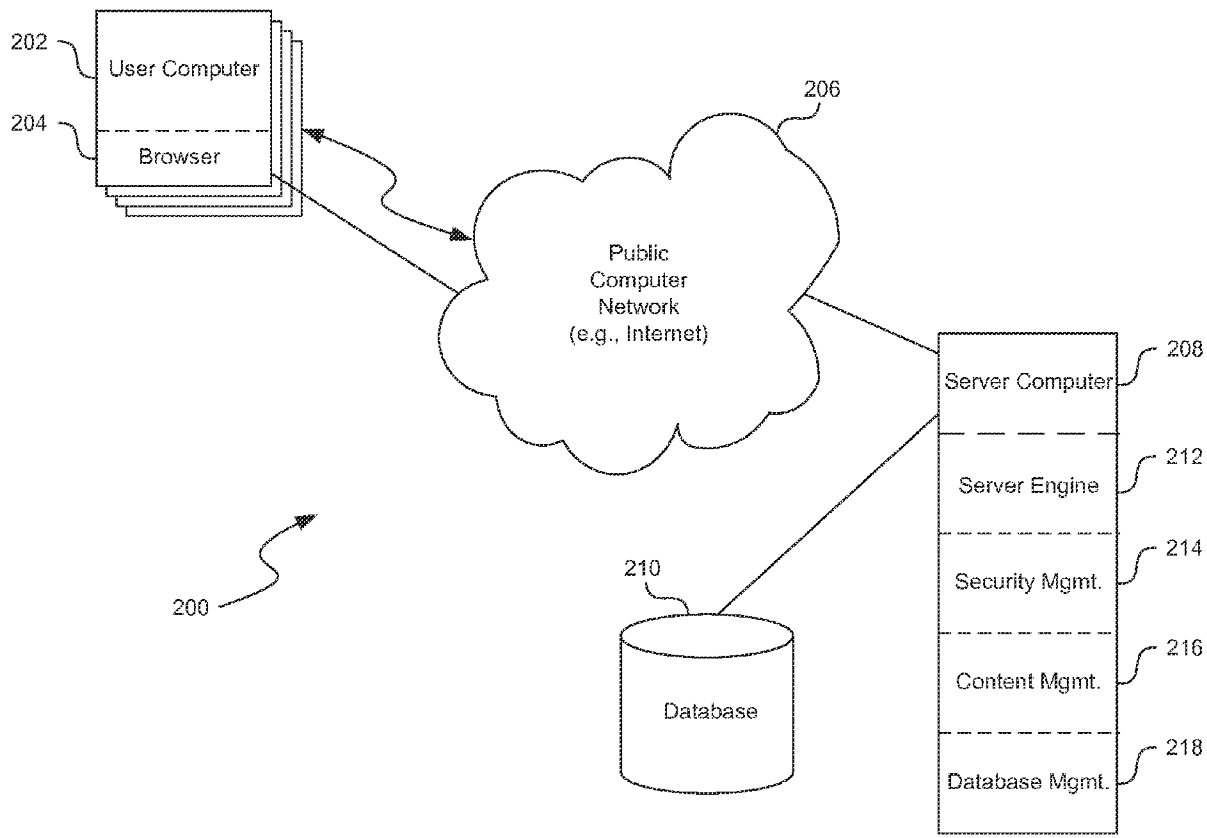

202
User Computer
204
Browser
206
Public
Computer
Network
(e.g., Internet)
208
Server Computer
212
Server Engine
214
Security Mgmt.
216
Content Mgmt.
218
Database Mgmt.
210
Database
200

FIG. 2

Asset Risk Profile 302

Risk Indicators 306

① **Asset A**: 304a
- Location (Public-Internet/Private-LAN/DMZ)
- Operating Sys (version, etc.)
- Known vulnerabilities (existing exploits)
- Future vulnerabilities (likelihood based on historical analysis-window 75% than Linux
- etc.
- Risk Assessment 308

② **Asset B** 304b

...

③ **Asset** n 304n

FIG. 3A

Asset Damage Profile 312

Damage Indicators 316

① **Asset A** 304a
- Data stored (credit card vs. webpages)
- Hardware (failovers operational?)
- Down time
- Reputation (and other intangibles)
- etc.
- Damage Assessment

② **Asset B** 304b

...

③ **Asset n** 304n

FIG. 3B

Company Risk Profile(s) 322

① **Company A:** 324a

Company Indicators 326

- Capital Investment (how much do they want to spend?)
- Risk tolerance (low, med, high—it's a subject based on customer)
- # of assets
- # of security measures (do they have a NOC/security team/Disaster Recovery Plan?)
- # of employees (could be an internal attack)
- Public vs. Private Co. (are they high profile)
- Line of business (Big Co. vs. Small Co.)
- History of Attacks
- etc.
- Company Risk Assessment 328

② **Company B:** 324b

...

③ **Company n:** 324c

FIG. 3C

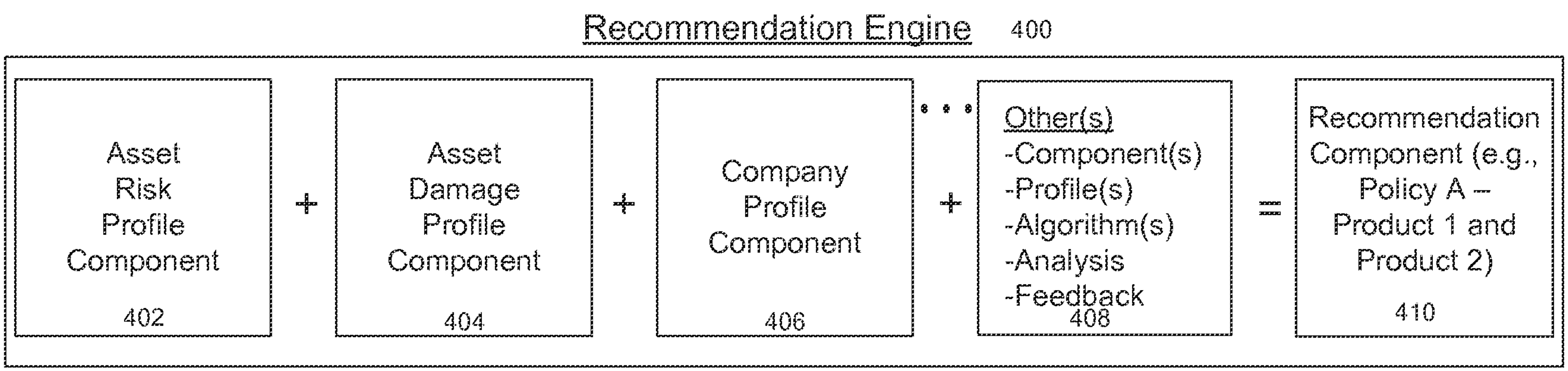

Recommendation Engine 400
Asset Risk Profile Component 402
+
Asset Damage Profile Component 404
+
Company Profile Component 406
+
Other(s)
-Component(s)
-Profile(s)
-Algorithm(s)
-Analysis
-Feedback
408
=
Recommendation Component (e.g., Policy A – Product 1 and Product 2)
410

FIG. 4

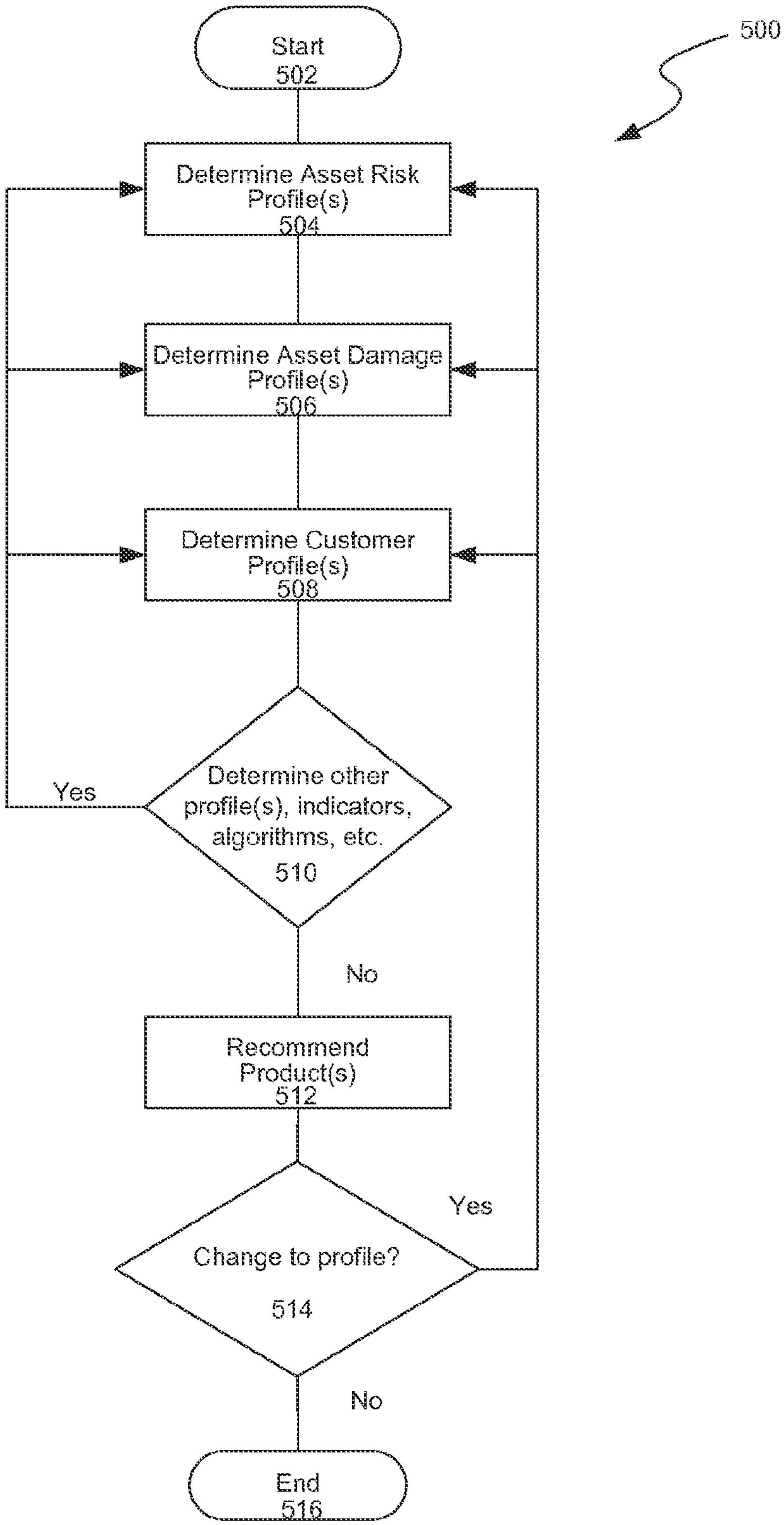

500
Start
502
Determine Asset Risk Profile(s)
504
Determine Asset Damage Profile(s)
506
Determine Customer Profile(s)
508
Determine other profile(s), indicators, algorithms, etc.
510
Yes
No
Recommend Product(s)
512
Change to profile?
514
Yes
No
End
516

FIG. 5

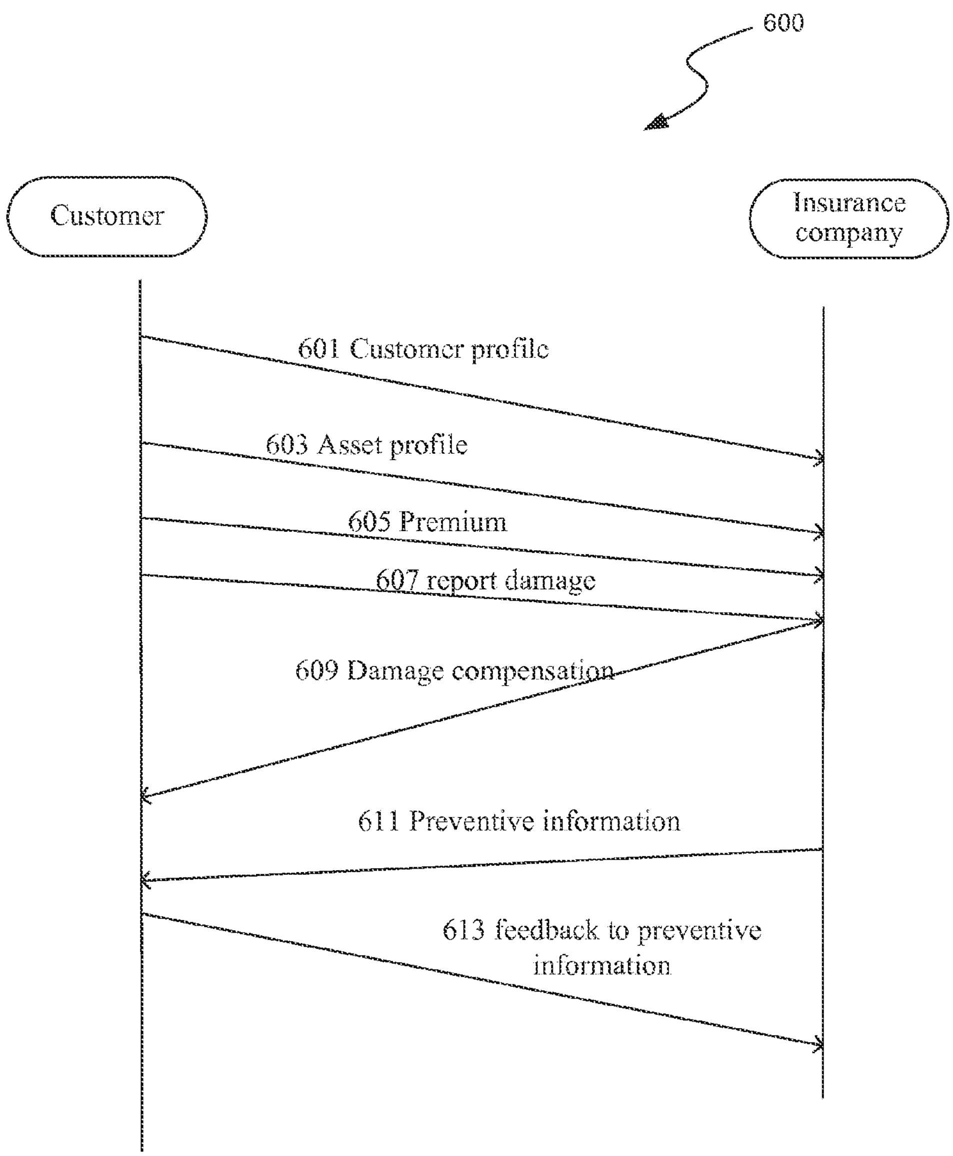

600
Customer
Insurance company
601 Customer profile
603 Asset profile
605 Premium
607 report damage
609 Damage compensation
611 Preventive information
613 feedback to preventive information

FIG. 6

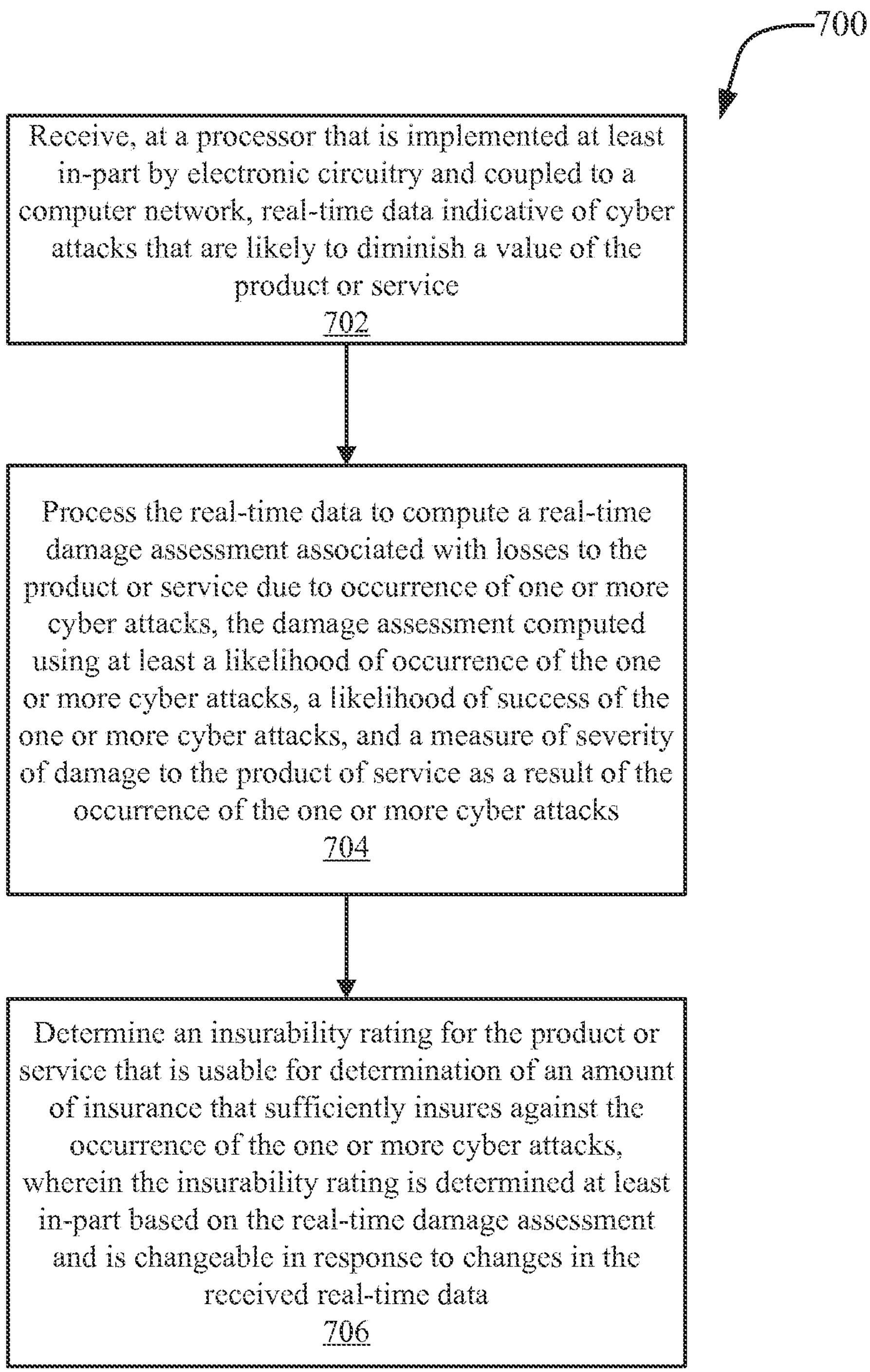

700
Receive, at a processor that is implemented at least in-part by electronic circuitry and coupled to a computer network, real-time data indicative of cyber attacks that are likely to diminish a value of the product or service
702
Process the real-time data to compute a real-time damage assessment associated with losses to the product or service due to occurrence of one or more cyber attacks, the damage assessment computed using at least a likelihood of occurrence of the one or more cyber attacks, a likelihood of success of the one or more cyber attacks, and a measure of severity of damage to the product of service as a result of the occurrence of the one or more cyber attacks
704
Determine an insurability rating for the product or service that is usable for determination of an amount of insurance that sufficiently insures against the occurrence of the one or more cyber attacks, wherein the insurability rating is determined at least in-part based on the real-time damage assessment and is changeable in response to changes in the received real-time data
706

FIG. 7

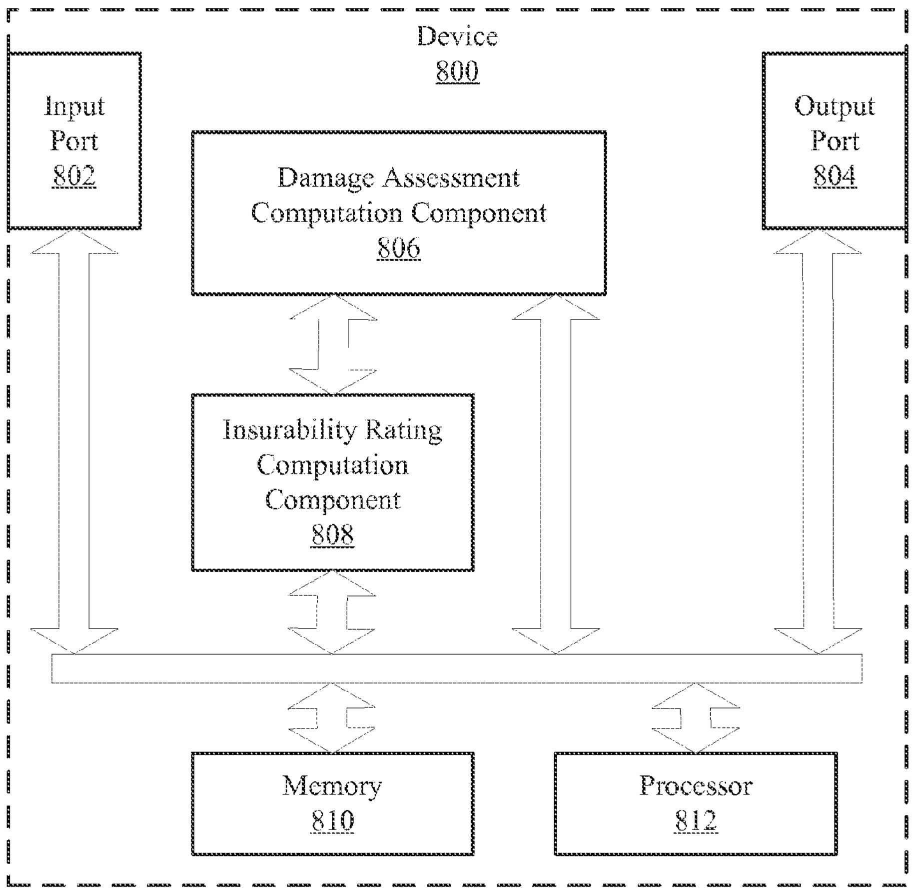

Device
800
Input
Port
802
Output
Port
804
Damage Assessment
Computation Component
806
Insurability Rating
Computation
Component
808
Memory
810
Processor
812

FIG. 8

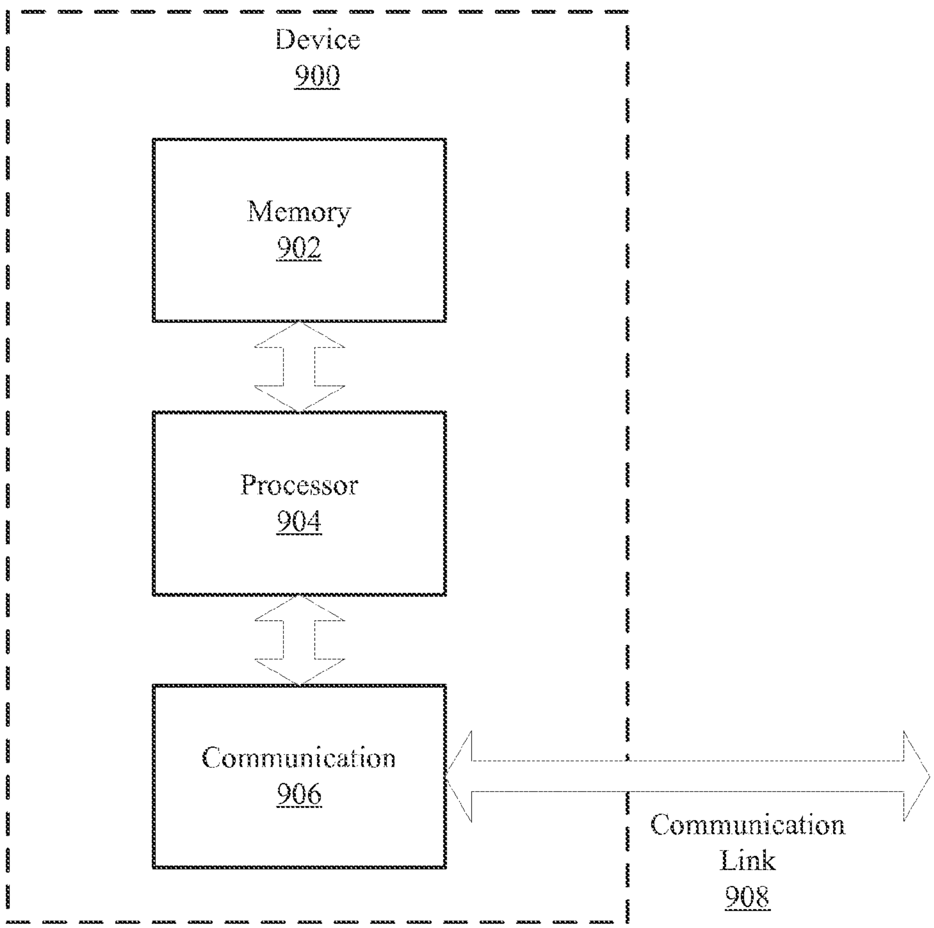

Device
900
Memory
902
Processor
904
Communication
906
Communication
Link
908

FIG. 9

DYNAMIC SECURITY RATING FOR CYBER INSURANCE PRODUCTS

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This patent application claims priority to U.S. Provisional Application No. 62/066,716, filed Oct. 21, 2014. The entire content of the before-mentioned provisional patent application is incorporated by reference as part of the disclosure of this application.

TECHNICAL FIELD

[0002] The present disclosure relates generally to systems, apparatuses, and methods and computer program that are stored on non-transitory storage media (collectively referred to as the "technology") related to determining a company's vulnerability to a cyber security-related attack ("cyber attack") and, based on the level of vulnerability, determining tailored cyber insurance policies and/or products to insure against the cyber attack.

BACKGROUND

[0003] This section is intended to provide a background or context to the disclosed embodiments that are recited in the claims. The description herein may include concepts that could be pursued, but are not necessarily ones that have been previously conceived or pursued. Therefore, unless otherwise indicated herein, what is described in this section is not prior art to the description and claims in this application and is not admitted to be prior art by inclusion in this section.

[0004] Insurance is a form of risk management tool primarily used by individuals, businesses, and other organizations to hedge against the risk of a contingent, uncertain loss that they can't or don't want to bear alone. An insured, or policyholder, can buy an insurance policy from an insurer, or insurance carrier, for an amount of money, called the premium, for a certain amount of insurance coverage specified by an insurance policy. Traditionally, insurance policies available to cover losses from business may be classified as: (1) business personal insurance policies to cover first-party losses; (2) business interruption policies; (3) commercial general liability or umbrella liability insurance policies, to cover liability for damages to third parties; and (4) errors and omissions insurance to cover the company's officers. These traditional insurance policies were designed to cover the traditional perils of fires, floods, and other forces of nature.

[0005] In the last half a century, computers have become an integrated part of life for any individuals and organizations. As organizations become more dependent on their networked computer assets, they become more vulnerable to harm from increasing frequent and damaging attacks made possible by computers. Since traditional insurance policies are normally written before the advent of the Internet, they do not expressly cover new computer related risks. Cyber insurance is a specialty insurance product that covers losses associated with a company's information assets including computer generated, stored, and processed information. Cyber insurance may become part of the overall solution to computer network and system security, which becomes more and more important due to the increasing number of virus attacks, hacker assaults, and other IT security incidents. However, due to the ever-changing nature of cyber security and cyber vulnerabilities, traditional insurance or even cyber insurance policies and associated premiums do not adequately correspond to the level of risk that is associated with a computer asset.

SUMMARY OF CERTAIN EMBODIMENTS

[0006] The disclosed technology relates to determination one or more cyber insurance policies, products and/or ratings based on processing of real-time information related to cyber attacks on one or more of computing assets that are coupled to a computer network.

[0007] One aspect of the technology relates to a method for producing insurability ratings for a product or service. The method includes receiving, at a processor that is implemented at least in-part by electronic circuitry and coupled to a computer network, real-time data indicative of cyber attacks that are likely to diminish a value of the product or service. The method further includes using the processor to process the real-time data to compute a real-time damage assessment associated with losses to the product or service due to occurrence of one or more cyber-attacks. The damage assessment is computed using at least a likelihood of occurrence of the one or more cyber attacks, a likelihood of success of the one or more cyber attacks, and a measure of severity of damage to the product of service as a result of the occurrence of the one or more cyber attacks. The above noted method also includes using the processor to determine an insurability rating for the product or service that is usable for determination of an amount of insurance that sufficiently insures against the occurrence of the one or more cyber attacks. The insurability rating is determined at least in-part based on the real-time damage assessment and is changeable in response to changes in the received real-time data.

[0008] In one exemplary embodiment, the method further includes using the insurability rating to produce an insurance premium value for the product or service. In another exemplary embodiment, the real-time damage assessment is computed on an on-going basis based on changes in the real-time data with a time granularity of 1 micro second or less. In yet another exemplary embodiment, the insurability rating is produced at least in-part by processing the real-time damage assessment over a pre-determined time interval and determining a statistical value associated with a plurality of insurability rating values over the pre-determined time interval. In some embodiments, the statistical value is an average of the plurality of insurability rating values over the pre-determined time interval. In some exemplary embodiments, the statistical value is a weighted average of the plurality of insurability rating values over the pre-determined time interval, and insurability rating values that correspond to later time instances within the predetermined time interval are assigned a larger weight compared to insurability rating values that correspond to earlier time instances within the predetermined time interval. In some example embodiments, the pre-determined time interval is one of: one hour, one day, one week or one month.

[0009] According to one exemplary embodiment, the above noted method further includes determining at least one additional insurability rating based on the real-time data, where one of the insurability rating or the additional insurability rating corresponds to a short-term insurability rating, and the other of the insurability rating or the additional insurability rating corresponds to a long-term insurability rating. In some exemplary embodiments, the short-term insurability rating corresponds to a time period that is in the range of one hour to one day, and the long-term insurability rating corresponds to a time period that is greater than one day and up to

one month. In still another exemplary embodiment, the real-time damage assessment is computed using a weighted average technique that assigns a first weight to the likelihood of occurrence of the one or more cyber attacks, a second weight to the likelihood of success of the one or more cyber attacks, and a third weight to the measure of severity of damage to the product of service. In yet another exemplary embodiment, each of the likelihood of occurrence of the one or more cyber attacks, the likelihood of success of the one or more cyber attacks, and the measure of severity of damage to the product of service is determined using historical information associated with previously launched cyber attacks against the products or the service. For example, the historical information can include one or more of: a number of previous cyber attacks against the product or service, a rate of success of previous cyber attacks against the product or service, an amount of damage to the service or product caused by a previous cyber attack, or a frequency of occurrence of cyber attacks against other entities that offer products or services that are similar to the product and service.

[0010] In one exemplary embodiment, the likelihood of occurrence of the one or more cyber attacks is produced by analyzing data associated with patterns of cyber activity over a plurality of data networks in real-time. In some embodiments, the patterns of cyber activity are indicative of cyber attacks on other organizations with network connectivity. In another exemplary embodiment, the insurability rating is determined using an inverse proportionality relationship with respect to the real-time damage assessment. In yet another exemplary embodiment, the insurability rating is determined based in-part on existing cybersecurity countermeasures that are deployed to protect computers, networks or storage units that participate in storage, production or distribution of the product or service. In some embodiments, the insurability rating is modified based on changes in the cybersecurity countermeasures deployed to protect computers, networks or storage units that participate in storage, production or distribution of the product or service.

[0011] In another exemplary embodiment, the above noted method further includes providing one or more of the following to an entity that is interested in obtaining or maintaining insurance coverage for the product or service: (a) information regarding the real-time damage, (b) information regarding the likelihood of occurrence of the one or more cyber attacks, (c) information regarding the likelihood of success of the one or more cyber attacks, (d) information regarding the measure of severity of damage to the product of service as a result of the occurrence of the one or more cyber attacks, (e) a recommendation for obtaining additional cybersecurity countermeasures, or (f) a particular cybersecurity countermeasure.

[0012] Another aspect of the technology relates to a computer program product, embodied on one or more non-transitory computer media, that includes program code for receiving real-time data from a computer network at a processor that is implemented at least in-part by electronic circuitry, where the real-time data is indicative of cyber attacks that are likely to diminish a value of the product or service. The computer program product further includes program code for processing by the processor the real-time data to compute real-time damage assessment associated with losses to the product or service due to occurrence of one or more cyber-attacks, where the damage assessment is computed using at least a likelihood of occurrence of the one or more cyber attacks, a likelihood of success of the one or more cyber attacks, and a measure of severity of damage to the product of service as a result of the occurrence of the one or more cyber attacks. The computer program product further includes program code for determining by the processor an insurability rating for the product or service that is usable for determination of an amount of insurance that sufficiently insures against the occurrence of the one or more cyber attacks, where the insurability rating is determined at least in-part based on the real-time damage assessment and is changeable in response to changes in the received real-time data.

[0013] Another aspect of the technology relates to a device that includes a processor implemented using electronic circuitry, and a memory comprising processor executable code. The processor executable code, when executed by the processor, causes the device or the components of the device to receive real-time data indicative of cyber attacks that are likely to diminish a value of the product or service, and process the real-time data to compute a real-time damage assessment associated with losses to the product or service due to occurrence of one or more cyber-attacks. The damage assessment is computed using at least a likelihood of occurrence of the one or more cyber attacks, a likelihood of success of the one or more cyber attacks, and a measure of severity of damage to the product of service as a result of the occurrence of the one or more cyber attacks. The processor executable code, when executed by the processor, further causes the device or the components of the device to determine an insurability rating for the product or service that is usable for determination of an amount of insurance that sufficiently insures against the occurrence of the one or more cyber attacks, where the insurability rating is determined at least in-part based on the real-time damage assessment and is changeable in response to changes in the received real-time data.

[0014] Another aspect of the technology relates to a system for determining insurability rating of a service or product that includes a server device coupled to a computer network to receive real-time data indicative of cyber attacks that are likely to diminish a value of the product or service and to produce an insurance premium estimate based at least in-part on the received real-time data. The system also includes a client device coupled the computer network to receive the insurance premium estimate produced by the server device. The server device uses the real-time data to compute a real-time damage assessment associated with losses to the product or service due to occurrence of one or more cyber-attacks, where the damage assessment is computed using at least a likelihood of occurrence of the one or more cyber attacks, a likelihood of success of the one or more cyber attacks, and a measure of severity of damage to the product of service as a result of the occurrence of the one or more cyber attacks. The sever device determines an insurability rating for the product or service that is usable for determination of an amount of insurance that sufficiently insures against the occurrence of the one or more cyber attacks, where the insurability rating is determined at least in-part based on the real-time damage assessment and is changeable in response to changes in the received real-time data.

BRIEF DESCRIPTION OF THE DRAWINGS

[0015] FIG. **1**. is a block diagram of a basic and suitable computer that may employ aspects of the described technology.

[0016] FIG. **2**. is a block diagram illustrating a simple, yet suitable system in which aspects of the described technology may operate in a networked computer environment.

[0017] FIG. **3**A illustrates an exemplary asset risk profile that may employ aspects of the described technology.

[0018] FIG. **3**B illustrates an exemplary asset damage profile that may employ aspects of the described technology.

[0019] FIG. **3**C illustrates an exemplary company risk profile that may employ aspects of the described technology.

[0020] FIG. **4** illustrates a block diagram of an exemplary device that can be implemented as part of the disclosed devices and systems.

[0021] FIG. **5** illustrates a flow diagram for determining cyber insurance based on various profiles in accordance with an exemplary embodiment.

[0022] FIG. **6** illustrates a flow diagram of communications between a customer and an insurance company in accordance with an exemplary embodiment.

[0023] FIG. **7** illustrates a set of operations that can be carried out to determine an insurability rating for a product or a service in accordance with an exemplary embodiment.

[0024] FIG. **8** illustrates some of the components of a device **1000** that can operate to produce an insurability rating in accordance with an exemplary embodiment

[0025] FIG. **9** illustrates a block diagram of a device that can be implemented as part of the disclosed devices and systems.

DETAILED DESCRIPTION

[0026] In the following description, for purposes of explanation and not limitation, details and descriptions are set forth in order to provide a thorough understanding of the disclosed embodiments. However, it will be apparent to those skilled in the art that the present invention may be practiced in other embodiments that depart from these details and descriptions. Additionally, in the subject description, the word "exemplary" is used to mean serving as an example, instance, or illustration. Any embodiment or design described herein as "exemplary" is not necessarily to be construed as preferred or advantageous over other embodiments or designs. Rather, use of the word exemplary is intended to present concepts in a concrete manner.

[0027] Cyber insurance can, in principle, be an important risk-management tool for strengthening IT security and reliability for companies. There may be many parties involved in the cyber insurance industry including underwriters, agents, and clients, code writers, inspectors, and vendors of products and services, working together to provide the needed coverage for the policy holders.

[0028] In some cases, specialized policies can cover losses from computer viruses or other malicious code, destruction or theft of data, business interruption, denial of service, and/or liability resulting from e-commerce or other networked IT failures. In some other cases, insurance policies for cyber insurance may cover the cost of legal disputes arising from cyber attacks on the insurance policy holder's digital assets. In still other cases, cyber insurance policies may specifically exclude certain coverages such as to exclude coverage of "electronic data," "computer code," and other similar terms as tangible property.

[0029] For an insurance policy, the deductible may play an important role in managing cyber security risk. For example, the deducible amount may be a way of lowering the insurance company's risk since a higher deductible can reduce the amount for paying out on a claim. In particular, higher deductibles can be imposed for companies with greater cyber security risks, such as those companies with consistently lower investment in cyber security, with poor security controls or with inadequate IT staff, among other factors. From a risk management point of view, it is important for a company to understand that deductibles affect the premiums. A lower deductible can lead to a higher premium, and vice versa.

[0030] Premiums can vary according to specific situation and the amount of coverage, and can range from a few thousand dollars for base coverage for small businesses to several hundred thousand dollars for major corporations with comprehensive coverage. Premiums may depend on the individual company's security risk exposure and can vary substantially depending on the insurance provider. For example, the premiums may depend on the number of computers affected, company level dollar loss distribution, and the timing of the breach event. Premiums may also depend on the industry the company is operating in. For example, a company operating in the high-tech area may rely on computers more with more exposure to computer risks, which leads to a higher premium. A premium may further depend on the elements of the insurance contract, such as the settlement amount that is paid, the occurrence of the event covered by the contract, and the time when the settlement is paid.

[0031] Before issuing a cyber insurance policy, an insurance carrier may require audits by independent IT security consultants on a case-by case basis, depending on the risks to be covered and the policy limits sought. To this end, a cyber insurance underwriter may first ask prospective clients to complete an information security assessment that covers items such as: standard configurations with security documentation for firewalls, routers, and operating systems, information security policies, including password management, virus protection, encryption, and security training for employees, vulnerability monitoring and patch management, physical security and access controls, including remote access, privacy and confidentiality policies, backup and restoration provisions, business continuity planning, periodic testing of security controls, and outsourcing and other third-party security provisions.

[0032] Various parties of the cyber insurance industry, such as underwriters, agents, and clients, code writers, inspectors, and vendors of products and services, may interact using modern insurance information systems. An insurance information system may need wide functionality, including both traditional tasks of information systems like data processing and storing and more advanced functions that has been traditionally done by humans such as risk evaluation.

[0033] These tasks, while may have been sufficiently carried out for traditional insurance policies, suffer from major drawbacks in the realm of cyber insurance due to proliferation of online cyber attacks that can simultaneously and quickly breach many computer systems, databases and networks and result in loss of data, compromise of financial, medical or military secrets or assets. Therefore, there is an urgent need to continuously monitor and predict cyber space activities and relate those activities to risks to an insured (or insurable) product or service. Using such a real-time insurance assessment system benefits both the insured and the insurer by allowing a more accurate and realistic risk assessment to take place, as well as enabling the insurer to quickly alert the insured of impending attacks or existing security vulnerabilities. Further, such a system can be used to create offers for

clients and make insurance deals online, to process insurance cases automatically and to automate many other tasks.

[0034] In various embodiments, the technology determines one or more cyber insurance policies and/or products based on a company's real-time exposure to a cyber attack on one or more of its computing assets (e.g., a computer serving company data). The technology performs various security analysis techniques to explore, locate, and evaluate a company's assets for creating risk and damage assessments that are used to dynamically determine cyber insurance policies/products that are tailored to that company at that moment of time and, optionally, based on future projections. The technology can continuously or semi-continuously monitor the company's network for any changes to assets and, if changes are detected that could affect the company's exposure to a cyber attack, information associated with the detected changes is fed back to aspects of the technology that are configured to determine new/modified cyber insurance policies/products.

[0035] In various embodiments, the technology identifies computing assets' (e.g., computers, servers, mobile devices, databases, storage technology, cloud infrastructure, network appliances, intrusion detection systems (IDSs), firewalls, etc.) vulnerabilities that may be used in a cyber attack for exploiting resources (e.g., consumer data, such as credit card numbers) stored in or accessible to a company's network(s). Vulnerabilities are identified using various network security audit standards and technologies, such as the Payment Card Industry Data Security Standard (PCI DSS), other standard(s) and/or one or more penetration tests for analyzing assets for various vulnerabilities that may be exploited via internal and/or external cyber attacks. Security audits, in some embodiments, determine the feasibility of a particular set of real and/or potential attack vectors, identify higher-risk vulnerabilities that result from a combination of lower-risk vulnerabilities exploited in a particular sequence, assess the magnitude of potential business and operational impacts of successful attacks, test the ability of network defenders (e.g., security personal, firewalls, IDSs, etc.) to successfully detect and respond to the cyber attacks, and provide evidence to support increased investments in technology and insurance. Damage values are assigned to tangible (e.g., theft of credit card numbers) and/or intangible (e.g., reputation) losses associated with an occurrence of one or more cyber-attacks which could successfully exploit an assets' software and/or hardware vulnerabilities.

[0036] For example, the technology can determine that an asset storing trade secrets and credit card information has a higher economic damage value than a value associated with a redundant publically accessible webserver. Damage values are, in various embodiments, adjusted based on various damage indicators, such as the complexity and/or sophistication required to execute an exploit, availability of an exploit, a likelihood of the occurrence a cyber-attack, and/or likelihood of success of a cyber-attack. For example, an asset storing trade secrets can have an increased damage value if the asset is vulnerable to, e.g., more than one exploit, less complex exploits, and/or widely known exploits. Based at least on a damage value associated with an asset, the technology, in some embodiments, is configured to dynamically determine an amount of insurance for sufficiently insuring against the occurrence of the cyber-attack. In various embodiments, the technology automatically and periodically performs real-time security audits to continuously or semi-continuously reassess a company's vulnerability to new cyber threats and dynamically determine new damage values and, in response, corresponding new recommendations for insurance coverage.

[0037] In some embodiments, the technology is a computer program product or service, a device or a system configured with program code for receiving real-time data indicative of cyber attacks that are likely to diminish a value of the product or service. For example, the technology can leverage various databases, websites, the darknet, bit torrents, and/or other networks and data sources for determining known exploits and/or generate new or modify versions of known exploits. The program code is configured to process real-time data to compute a real-time damage assessment associated with losses for an occurrence of one or more cyber attacks. For example, the damage assessment can be computed using a likelihood of the occurrence of the one or more cyber attacks, a likelihood of success of the one or more cyber attacks, and a measure of severity of damage to the product or service as a result of the occurrence of the one or more cyber attacks. The program code, in various embodiments, is configured with technology that determines an insurability rating for the product or service for insuring against the cyber attacks. The insurability rating is usable for determination of an amount of insurance that sufficiently insures against the occurrence of the one or more cyber attacks, at least in-part based on the real-time damage indicator and is changeable in response to changes in the received real-time data.

[0038] In various embodiments, the technology determines asset risk assessments, asset damage assessments, and customer risk assessments. Assessments are snapshots of real-time asset and/or company behavior based on various indicators and expressed as simple values, such as a number, percentage, hash, etc. Each asset, in one or more embodiments, is associated with one or more profiles or other data structures ("profiles") that are associated with indicators that define asset and/or company characteristics and are used by the technology as variables for calculating assessment value. For example and as further described below, the technology can determine that an asset (e.g., a server) has a risk assessment of 8 out of 10 (i.e., 0.8) based on various indicators in that asset's profile, such as being a public server (i.e., a first indicator) operating using an older operating system and/or other software products (i.e., a second indicator) that has known vulnerabilities (i.e., a third indicator). That asset (e.g., the server described above) is also, in one or more embodiments, associated with a damage assessment, which is a measure of a company's estimated loss of capital and/or intangible losses (e.g., loss due to an adverse effect to company reputation) if the asset were compromised by a cyber-attack. Similar to the determination of the risk assessment, a damage assessment for the server mentioned above could be, for example, 3 out of 10 (i.e., 0.3) because the server stores lower valued webpages and, if compromised, would not negatively affect the company's reputation. By determining respective snapshots associated with risk and damage, the technology can efficiently and quickly identify, in real-time, assets at most risk of being compromised, associated losses and, in response, recommend insurance policies based on a company's unique circumstance and preferences. In some embodiments, multiple risk assessments are combined into a single meta-value that represents some or all of a company's assessments (e.g., a company's subsidiaries, different departments, or portions of a network).

[0039] In some embodiments, a profile is referenced for determining a company risk assessment, i.e., the level of risk associated with a specific company based on, for example, various indicators such as an amount of capital the company is willing to invest in cyber insurance, its risk tolerance, the number of assets to insure, existing security measures (e.g., an implemented network operating center (NOC), staff, and/or disaster recovery protocols), whether the company is high profile, the company's business, any history of attacks and their success, etc. Company risk profiles are automatically and/or manually determined and, in various embodiments, include a company's threshold tolerance for preventing and/or insuring against a determined level of financial loss (e.g., up to $2 million USD) as a result of the occurrence of the cyber-attack on an asset.

[0040] In one more embodiments, based on one or more indicators of the asset risk profile, asset damage profile, and/or company risk profile, the technology determines one or more insurance policies/products specific to the company. In various embodiments, the technology continuously, or on a schedule, updates the profiles based on changes to the assets or company (e.g., a new asset is added or an asset is recommissioned, critical data is moved, new vulnerabilities are discovered, etc.). In response to the changes to one or more of the profiles, the technology dynamically and automatically determines a new policy tailored to the changed profiles. This feedback technique allows the company to efficiently and comprehensively understand, in real time, where it has vulnerabilities and how best to insure against losses.

[0041] Referring to FIG. **1**, an exemplary embodiment of the described technology employs a computer **100**, such as a personal computer or workstation, having one or more processors **101** coupled to one or more user input devices **102** and data storage devices **104**. The computer **100** is also coupled to at least one output device such as a display device **106** and one or more optional additional output devices **108** (e.g., printer, plotter, speakers, tactile or olfactory output devices, etc.). The computer **100** may be coupled to external computers, such as via an optional network connection **110**, a wireless transceiver **112**, or both.

[0042] The input devices **102** may include a keyboard, a pointing device such as a mouse, and described technology for receiving human voice, touch, and/or sight (e.g., a microphone, a touch screen, and/or smart glasses). Other input devices are possible such as a joystick, pen, game pad, scanner, digital camera, video camera, and the like. The data storage devices **104** may include any type of computer-readable media that can store data accessible by the computer **100**, such as magnetic hard and floppy disk drives, optical disk drives, magnetic cassettes, tape drives, flash memory cards, digital video disks (DVDs), Bernoulli cartridges, RAMs, ROMs, smart cards, etc. Indeed, any medium for storing or transmitting computer-readable instructions and data may be employed, including a connection port to or node on a network, such as a LAN, WAN, or the Internet (not shown in FIG. **1**).

[0043] Aspects of the described technology may be practiced in a variety of other computing environments. For example, referring to FIG. **2**, a distributed computing environment with a network interface includes one or more user computers **202** (e.g., mobile devices, desktops, servers, etc.) in a system **200**, each of which can include a graphical user interface (GUI) program component (e.g., a thin client component) **204** that permits the user computer **202** to access and exchange data, such as network and/or security data, with a network **206** such as a LAN or the Internet, including web sites, ftp sites, live feeds, and data repositories within a portion of the network **206**. The user computers **202** may be substantially similar to the computer described above with respect to FIG. **1**. The user computers **202** may be personal computers (PCs) or mobile devices, such as laptops, mobile phones, or tablets. The user computers **202** may connect to the network **206** wirelessly or through the use of a wired connection. Wireless connectivity may include any forms of wireless technology, such as a radio access technology used in wireless LANs or mobile standards such as 2G/3G/4G/LTE. The user computers **202** may include other program components, such as a filter component, an operating system, one or more application programs (e.g., security applications, word processing applications, spreadsheet applications, or Internet-enabled applications), and the like. The user computers **202** may be general-purpose devices that can be programmed to run various types of applications, or they may be single-purpose devices optimized or limited to a particular function or class of functions. More importantly, any application program for providing a graphical user interface to users may be employed, as described in detail below. For example, a mobile application or "app" has been contemplated, such as one used in Apple's® iPhone® or iPad® products, Microsoft® products, Nokia® products, or Android®-based products.

[0044] At least one server computer **208**, coupled to the network **206**, performs some or all of the functions for receiving, routing, and storing of electronic messages, such as security data, web pages, audio signals, electronic images, and/or other data. While the Internet is shown, a private network, such as an intranet, may be preferred in some applications. The network may have a client-server architecture, in which a computer is dedicated to serving other client computers, or it may have other architectures, such as a peer-to-peer, in which one or more computers serve simultaneously as servers and clients. A database or databases **210**, coupled to the server computer(s), store some content (e.g., security-related data) exchanged between the user computers; however, content may be stored in a flat or semi-structured file that is local to or remote of the server computer **208**. The server computer(s), including the database(s), may employ security measures to inhibit malicious attacks on the system and to preserve the integrity of the messages and data stored therein (e.g., firewall systems, secure socket layers (SSL), password protection schemes, encryption, and the like).

[0045] The server computer **208** may include a server engine **212**, a security management component **214**, an insurance management component **216**, and a database management component **218**. The server engine **212** performs basic processing and operating system level tasks. The security management component(s) **214** handle creation, streaming, processing and/or routing of networking and/or security data. Security management components **214**, in various embodiments, includes other components and/or technology, such as an asset risk component, asset damage component, company risk component and/or other components and/or assessment technologies, described below. Users may access the server computer **208** by means of a network path associated therewith. The insurance management component **216** handles processes and technologies that support the collection, managing, and publishing of insurance and/or cyber-related data and information, and other data. The database management

component **218** includes storage and retrieval tasks with respect to the database, queries to the database, and storage of data. In some embodiments, multiple server computers **208** each having one or more of the components **212-218** may be utilized. In general, the user computer **202** receives data input by the user and transmits such input data to the server computer **208**. The server computer **208** then queries the database **210**, retrieves requested pages, performs computations and/or provides output data back to the user computer **202**, typically for visual display to the user. Additionally, or alternatively, the user computers **202** may automatically, and/or based on user computers' **202** settings/preferences, receive various information, such as alerts, updates, cyber security assessments, cyber security programs, etc., from the server computer **208**.

[0046] FIG. **3**A illustrates one example of an asset risk profile **302**. An asset risk profile **302** includes various asset descriptions **304***a*-**304***n* each having one or more indicators **306** for defining attributes which may affect that asset's risk assessment **308** (e.g., whether the asset has a high, medium, or low risk rating). For example, Asset A **304***a* includes various indicators **306**, such as the physical location of the asset, software operating on the asset (e.g., a version of an operating system, such as a Windows 8®), known vulnerabilities (e.g., a virus or rootkit active on the asset), unknown or future vulnerabilities (e.g., a yet to be released exploit that is programmed for the asset's operating system), etc. As an additional example, an asset risk profile **302** may specify various risk indicators descriptive of the asset's hardware (e.g., an Intel-based server, 1 Terabyte Western Digital hard drive, vendor-specific network interface card (NIC)), and/or software/services (e.g., a command shell with super user privileges)), etc. The technology can determine, at least based on one or more risk assessments **308** (e.g., a value determined via the technology's implementation of a weighted-value-based algorithm or other algorithm), a representative multiple of the risk indicators **306**. For example, the technology can determine that an asset with an old version of an operating system having known vulnerabilities running moderately easy to hack NIC drivers has a high risk assessment value (e.g., 0.95) and a modern, recently updated asset has a lower risk assessment value (e.g., 0.15).

[0047] Risk indicators **306** can define virtually any type of information that may affect an asset's exploitation and values of risk indicators **306** are specific to an asset. In other words, different assets, e.g., Asset B **304***b* and Asset n **304***n*, can have different indicators and/or types of indicators than the indicators **306** associated with Asset A **304***a*. As mentioned above, risk indicators **306** are used by the technology, in one or more embodiments, to determine a risk assessment **308**, based on one or more predetermined algorithms. The risk assessment **308** is a snapshot of real-time risk to an asset (e.g., Asset A **304***a*) based on the indicators **306** that, in some embodiments, are being continuously or semi-continuously updated via new or continuing security assessments of the company's network. In other words, as assets change (e.g., an asset's operating system is updated) a new risk assessment **308** is automatically and/or manually determined.

[0048] FIG. **3**B illustrates one example of an asset damage profile **312** for an asset (e.g., Asset **304***a*). Asset damage profile **312** is associated with damage indicators **316** for each of a company's assets (e.g., Asset **304***a*-**304***n*), which may indicate a potential loss (i.e., a tangible or intangible loss) to a company if the asset (e.g., Asset **304***a*) were compromised by a cyber attack. For example, Asset **304***a*, discussed above in reference to asset risk profile **302**, includes various damage indicators **316** for determining, by the technology, a damage assessment **318**, based on one or more predetermined algorithms. Damage indicators **316** include virtually any information and any type of information that may affect a loss to a company if the asset (e.g., Asset **304***a*) is compromised and can include, for example, a data type indicator representative of the data being stored (e.g., credit cards, trade secrets or webpages), hardware cost indicator (e.g., the cost of purchasing new hardware), down time loss indicator, loss indicator associated with company reputation (e.g., public and/or shareholders), etc. The damage assessment **318** is a snapshot of real-time damage to a company (e.g., tangible and intangible losses) if a particular asset (e.g., Asset A **304***a*) were to be compromised. In some embodiments, similar to the feedback technique described for the asset risk profile **302**, damage assessments **318** can be continuously or semi-continuously updated via new or continuing security assessments of the company's network. In other words, as the network changes (e.g., an asset, such as Asset **304***a*, switches from storing financial security information to storing publicly available emails address) a new damage assessment **308** is determined automatically and/or manually for that asset (e.g., Asset **304***a*).

[0049] FIG. **3**C illustrates one example of a company risk profile **322** for defining various company attributes and/or preferences, based on one or more various company indicators **326**. The technology, in one or more embodiments, references a company's (e.g., Company A **324***a*, Company B **324***b*, and/or Company n **324***n*) indicators **326** for determining a company's general risk, based on factors other than indicators **328**, which are specific to a particular asset (e.g., Asset A **304***a*). For example, the technology determines a risk assessment **320** for the company based on various company indicator's **326** unique to that company, such as the company's public exposure, profits, global reach, investments, line (s) of business, number and sophistication of employees/customers/clients, existing security measures implemented by the company, total number of potentially exploitable assets, history of cyber attacks, etc. Other indicators, such as company's level of tolerance of a cyber attack and the company's capital investment commitment for insuring against cyber-attacks are used by the technology in determining one or more insurance policies/products tailored to the company's situation and preferences.

[0050] FIG. **4** illustrates one example of an engine **400** used by the technology to determine and/or recommend to a company one or more cyber insurance policies tailored to that company's asset, damage and/or company profiles. Engine **400** includes various components **402-410**, such as an asset risk profile component **402**, an asset damage profile component **404**, and a company risk profile component **406** and other optional component(s) **408** (e.g., other profiles, algorithms, analysis, feedback, etc.) for determining, by recommendation component **410**, one or more cyber insurance polices (e.g., a policy that includes cyber insurance Products **1** and **2**). As referenced in the illustration for FIG. **4**, the technology determines and/or recommends one or more insurance policies and/or products based on features of one or more of the asset risk profile **302** (e.g., a risk assessment **308** and/or risk indicators **306**), asset damage profile **312** (e.g., damage assessment **318** and/or damage indicators **316**) and company risk profile **322** (e.g., company risk assessment **328**

and/or company indicators **326**). Based on the one or more features of components **402-408**, the technology determines and/or recommends cyber insurance policies/products by, for example, referencing a database or other data storing insurance information (e.g., premium, coverage amounts/percentages, terms, etc.) and calculating, via the recommendation component **410**, preferred policies/products for the company's specific requirements and preferences.

[0051] One aspect of the disclosed technology relates to a computer-implemented cyber attack assessment method that includes identifying one or more software vulnerabilities for exploiting resources on one or more computing devices, assigning a damage value associated with tangible and intangible losses for an occurrence of one or more cyber attacks exploiting the one or more software vulnerabilities, and dynamically determining an amount of insurance for sufficiently insuring against the occurrence of the one or more cyber attacks exploiting the one or more software vulnerabilities, wherein the amount of insurance is at least based on the damage value. In some embodiments, such a method further includes periodically determining a new amount of insurance based on identifying one or more new software vulnerabilities for exploiting resources on the one or more computing devices.

[0052] In another aspect of the technology, a computer-readable storage device stores instructions that, upon execution by a processor of a computing system, cause the computing system to perform a method for insuring against cyber attacks within a network. The method includes determining an asset profile for a target asset, and assigning a risk rating to the target asset, wherein the risk rating is a measure of: (a) vulnerability of the target asset to a present or future cyber attack and (b) a cost associated with an occurrence of the cyber attack on the target asset. Such a method further includes identifying a customer risk profile associated with preventing the occurrence of the cyber attack on the target asset, and dynamically determining one or more financial instruments for insuring against the occurrence of the cyber attacked on the target asset, based at least on the risk rating and the customer risk profile.

[0053] In some embodiments, the asset profile includes characteristics descriptive of software products and data installed on the target asset. In some embodiments, the customer risk profile includes a threshold tolerance for preventing a determined level of financial loss as a result of the occurrence of the cyber attack on the target asset. In some embodiments, the one or more financial instruments insure against the occurrence of the cyber attack based on the determined level of financial loss. In some embodiments, the above noted method further includes dynamically and periodically determining one or more new vulnerabilities and, in response to determining the one or more new vulnerabilities, assigning a new risk rating and determining one or more new financial instruments for insuring against an occurrence of a new cyber attack based on the one or more new vulnerabilities.

[0054] FIG. **5** illustrates a flow diagram **500** for determining a company's risk of a cyber attack and recommending a cyber insurance policy based on the determined risk. The flow starts at **502** and, at **504**, the technology determines (e.g., via a security assessment) a network's vulnerability to cyber-attacks and stores results of the assessment in a assets risk profile **302**. At **506**, the technology determines one or more asset damage profiles **312** for each of the one or more assets defined in the asset risk profile **302** and, at **508**, in some embodiments, defines indicators in the customer risk profile **322**. If there are additional profiles and/or indicators then, at **510**, the flow returns to **504**, **506**, and/or **508**. Otherwise, the flow continues to **512** where the technology determines and/or recommends one or more cyber insurance policies/products for insuring against the possibility of a cyber-attack, based on the results of operations at **504-508**. At **514**, if there has been a change to the assets and/or customer preferences, the flow returns to **504**, **506**, and/or **508**. Otherwise, the flow ends at **516**. Further description, embodiments and/or implementations of policies, indicators, and assessments may be found in reference to one or more of the remaining figures.

[0055] FIG. **6** illustrates a flow diagram **600** of communications between a customer/company ("customer") and an insurance company in accordance with an exemplary embodiment. At **601**, a customer provides a customer profile to the insurance company. At **603**, the customer provides an asset profile to the insurance company. At **605**, the customer pays the premium to the insurance company to buy a policy. At **607**, the customer reports certain damages to the insurance company. At **609**, the insurance company pays the customer a damage compensation based on the policy that was purchased as part of operation **605**. The insurance company may perform some verification and damage assessment before paying such damage compensation at **609**.

[0056] The complexity of the computer related security threats makes it hard for small companies to have the most updated information and the skills needed to cope with the ongoing and increasing threats faced every day in the world. Computer security personal are highly skilled, hard to find, and highly paid. Therefore it is unrealistic for small companies to be able to maintain the most up to up-to-date defenses against the ever increasing attacks on computer assets. The insurance company, on the other hand, has to hire the highly skilled computer security personal to perform the security analysis, to keep updated with the most recent attacks with new methods. Therefore the insurance company can play a preventive role on behalf of many small companies by sharing the computer security expertise, developing defense guidelines, and distributing such defense guidelines and strategies among the insured companies. In this way, the insurance company can bear, or share with the small companies, the costs associated with combatting computer security threats while providing better defenses against new attacks.

[0057] Referring again to FIG. **6**, at **611**, the insurance company may distribute preventive information to the customer so that the customer can be aware of the most recent attacks and the associated techniques for defending against such attacks. At **613**, the customer provides feedback based on the preventive information received from the insurance company, where the feedback may include the status report of the implementation results related to the preventive information distributed by the insurance company.

[0058] One aspect of the disclosed technology relates to determination of insurability of a product or service based on real-time cyber activity, which can lead to a determination of an insurance premium for the product or service. The insurability rating provides a measure as to insurability of the product or service. Examples of products or services include consumer data (e.g., credit card information, personal information) that is stored on a network-accessible storage unit, cloud computing resources that are provided to paying customers, social media services, financial information, financial services, and others. In the context of the disclosed examples,

a high insurability rating is commensurate with having a product or service that is easily insurable (e.g., there is a lower risk of damage to the product or service), whereas a low insurability indicates that there is a higher risk of damage to the product or service. It is however, understood that such an inverse correlation between the insurability rating and damage risk is merely provided for the sake of illustration, and other relationships (e.g., direct correlation) can also be used. The insurability rating can be a number or a range of numbers. For instance, in one implementation, the insurability rating is a number between 0 and 100, whereas in another implementation, the insurability rating is represented by high (e.g., ratings in range 80 to 100), medium (e.g., ratings in range 60 to 79) and low (e.g., ratings in range 0 to 59).

[0059] FIG. **7** illustrates a set of operations **700** that can be carried out to determine insurability rating for a product or a service in accordance with an exemplary embodiment. The operations **700** can be implemented using a computing system with network connectivity. Such a computing system includes a processor (e.g., a hardware implemented processor comprising electronic circuitry), memory, physical buses and interfaces that allows different components of the system to communicate with one another and with other devices that are connected to the computing device through a network. Referring to FIG. **7**, at **702**, real-time data indicative of cyber attacks that are likely to diminish a value of the product or service is received at a processor that is implemented at least in-part by electronic circuitry and coupled to a computer network. At **704**, the real-time data is processed to compute a real-time damage assessment associated with losses to the product or service in the event of one or more cyber attacks. The real-time damage assessment can be computed using at least a likelihood of occurrence of the one or more cyber attacks, a likelihood of success of the one or more cyber attacks, and a measure of severity of damage to the product of service as a result of the occurrence of the one or more cyber attacks. For example, a higher likelihood of cyber attack, a higher likelihood of the success of the cyber attack, and a higher severity measure of damage caused by such cyber attacks, each contribute to a higher computed real-time damage assessment.

[0060] Referring again to FIG. **7**, at **706**, an insurability rating for the product or service is determined. Such an insurability rating can be used to determine an amount of insurance that sufficiently insures against the occurrence of the one or more cyber attacks. The insurability rating is determined at least in-part based on the real-time damage assessment and is changeable in response to changes in the received real-time data.

[0061] The insurability rating can be used to produce an insurance premium value for the product or service. Such an insurance premium can also be affected by other factors, such as the length of relationship between the insurer and the organization or person that is seeking insurance (the "insured"), the insurance premiums offered by other insurers, existence of other insurance polices for the product or service, discounts based on the number of other products or services that are insured by the same insurer, and other factors.

[0062] One of the advantages of the disclosed technology relates to the use of real-time data that allows dynamic and up-to-date computation of the damage assessment based on cyber activities that are being continuously monitored. For instance, in one exemplary implementation, the real-time damage assessment is computed on an on-going basis based on changes in the real-time data with a time granularity of 1 micro second or less. Thus, through, for example, monitoring world-wide attacks on particular assets or organizations, the damage assessment can be updated almost instantaneously to allow certain mitigating actions to be triggered. A number or a range of numbers can represent the damage assessment. For instance, in one implementation, the damage assessment is a number between 0 and 100, whereas in another implementation, the damage assessment is represented by a set of three numbers indicative of high (e.g., ratings in range 80 to 100), medium (e.g., ratings in range 60 to 79) and low (e.g., ratings in range 0 to 59) values of the real-time damage assessment.

[0063] In one implementation, the real-time damage assessment is computed by an algorithm that uses a weighted average technique. This technique assigns a first weight to an indicator representative of a likelihood of the occurrence of the one or more cyber attacks, assigns a second weight to an indicator representative of a the likelihood of success of the one or more cyber attacks, and a third weight to an indicator representative of the measure of severity of damage to the product of service. The weights can be indicative of the importance of each of the associated indicators of likelihood and/or measure. Further, each of the likelihood of the occurrence of the one or more cyber attacks, the likelihood of success of the one or more cyber attacks, and the measure of severity of damage to the product of service can be determined using historical information associated with previously launched cyber attacks against the products or the service.

[0064] The historical information is typically obtained based on attacks, damages and success rates of previous cyber attacks. For example, the historical information can include a number of previous cyber attacks against the product or service, a rate of success of previous cyber attacks against the product or service, an amount of damage to the service or product caused by the previous cyber attack(s), or a frequency of occurrence of cyber attacks against other entities that offer products or services that are similar to the product and service. In one example, the damage caused by breach of financial data at one financial instruction is used to produce a measure of damage for another financial institution. The disclosed technology enables the likelihood of a cyber attack to be produced by analyzing the patterns of cyber activity over a large number of data networks, which can all be carried out in real-time as those evolve over time.

[0065] The damage assessment can be used to compute the insurability rating. In one example, computation of the insurability rating includes processing the real-time damage assessment over a pre-determined time interval and then determining a statistical value associated with several of the insurability rating values over that pre-determined time interval. An example of the statistical value is an average of several insurability rating values over the pre-determined time interval. In one variation, the statistical value is a weighted average of the plurality of insurability rating values over the pre-determined time interval. In this scenario, the weights can be assigned or determined using different techniques that would allow easy adaptation and correlation to the changes in the real-time data. For example, in computing the average value, insurability rating values that correspond to later time instances within the predetermined time interval are given a larger weight compared to the insurability rating values that correspond to earlier time instances within the predetermined time interval.

[0066] The choice of the pre-determined time interval is often left to the designer of the system and can be based on system capabilities and recourses, observed time-dependence of cyber activity patterns, importance of the product or service, and other factors. For example, the time interval can be set to be one hour, one day, one week or one month. The pre-determined time interval can also be set to an initial value, and can then be changed based on changes in the system resources, cyber activity patterns, customer requests, or other factors. It should be noted that in some instances it might be beneficial to compute more than one insurability rating so as to ascertain a trend in insurability rating over time, or for other reasons that facilitate the determination of the proper premium. For example, both a short-term and a long-term insurability rating can be computed, with the short-term insurability rating spanning a time period in the range of, e.g., one hour to one day, and the long-term insurability corresponding to a time period that is, e.g., greater than one day and up to one month.

[0067] In some implementations, the insurability rating is determined based in-part on the existing cybersecurity countermeasures that are being deployed to protect computers, networks or storage units that participate in storage, production or distribution of the product or service. Examples of such cyber security countermeasures include firewalls, anti-virus software, system alerts, fail-safe measures that, for example, limit the amount of loss to the product or service (e.g., cash withdrawal limits), biometric authorization protections and others administrative or physical security measures. In some implementations, the insurability rating is modified dynamically based on changes in cybersecurity countermeasures that are deployed to protect the assets. For example, upon a detection that deployed anti-virus software has expired or has become outdated, the insurability rating can correspondingly change to reflect a higher risk to the asset.

[0068] As noted in connection with operation **611** of FIG. **6**, certain information and/or cyber security countermeasures can be shared with an insured party upon a determination that indicates an elevated cyber security risk. For example, one or more of the following can be shared with an entity that is interested in obtaining or maintaining insurance coverage for the product or service: information regarding the real-time damage, information regarding the likelihood of the occurrence of the one or more cyber attacks, information regarding the likelihood of success of the one or more cyber attacks, information regarding the measure of severity of damage to the product of service as a result of the occurrence of the one or more cyber attacks, a recommendation for obtaining additional cybersecurity countermeasures, or a particular cybersecurity countermeasure.

[0069] FIG. **8** illustrates some of the components of a device **800** that can operate to produce an insurability rating in accordance with an exemplary embodiment. The device **800** includes an input port **802** and an output port **804** that allow the device **800** to receive/send data, commands or other signal from/to an outside entity. For example, the input port **802** or the output port **804** can be a serial port, parallel port, a USB port, a wireless connectivity port, an Ethernet port, or other types of input/output ports that are known in the art. In some implementations, the input port **802** and output port **804** may be part of communication component that provide wired and/or wireless communication capabilities in accordance with one or more communication protocols, and therefore they may comprise the proper transmitter/receiver, antennas, circuitry and ports, as well as the encoding/decoding capabilities that may be necessary for proper transmission and/or reception of data and other information.

[0070] The device **800** in FIG. **8** also includes a processor **812** and memory **810** that are in communication with each other and with other components of the device through, for example, busses, optical interconnects, wireless connections or other means of connectivity that allow the exchange of data and control signals. The processor **812** can, for example, be a microprocessor, a controller or other processing device that is known in the art. The memory **810** can be used to permanently or temporarily (e.g., as in a buffer) store data, program code, parameters or other information that can be used to configure and/or operate the device **800** or the components therein. The device **800** also includes a damage assessment computation component **806**, which is coupled to the input port **802** and is configured to receive data on an on-going basis (e.g., real-time data indicative of cyber activity) and compute a real-time damage assessment associated with losses to the product or service in the event of one or more cyber attacks.

[0071] The damage assessment computation component **806** can include sub-components (not shown) that parse the data received from the input port **802** or other device components, and route the appropriate data to other subcomponents (not shown) of the damage assessment computation component **806**. For example, a routing subcomponent (not shown) can sift the incoming data to identify and route the following types of data to an aggregation subcomponent: data indicative of a likelihood of the occurrence of the one or more cyber attacks, data a likelihood of success of the one or more cyber attacks, and data indicative of a measure of severity of damage to the product of service as a result of the occurrence of the one or more cyber attacks. The damage assessment computation component **806** can also include one or more subcomponents (e.g., an aggregation subcomponent) that are configured to assign weights, compute averages, and modify data to determine a damage assessment value or values.

[0072] The device **800** also includes an insurability rating computation component **808** that is coupled to the damage assessment computation component **806** and is configured to receive a damage assessment value or values and to determine an insurability rating for the product or service that is usable for determination of an amount of insurance that sufficiently insures against the occurrence of the one or more cyber attacks. The insurability rating computation component **808** is configured to receive the damage assessment values on a real-time basis and use them to produce and update insurability ratings in response to changes in the real-time data. The insurability rating computation component **808** can also include subcomponent (not shown) that are configured to assign weights, compute averages, and modify data to determine the insurability rating. The insurability ratings can be communicated to outside components (not shown) using the output port **804**. Examples of those outside components include a monitor, a storage device (e.g., RAM, Optical or Magnetic disks, etc.), a printer and a networked computing device.

[0073] It should be noted that to avoid clutter, FIG. **8** might not show all of the components of the device **800**, or all connections between the device components. For example, in instances where data compression is used to reduce the storage and transmission bandwidth of data that is received and processed by device **800**, the device **800** may include com-

ponents that are configures to decompress and decompress the data based on the specific compression/decompression algorithms (e.g., LZV, Run Length Encoding, PKZip, etc.). Similarly, in instances where data encryption is used to ensure the security of data (e.g., for the external data received by the device **800**, data transmitted by the device **800** to outside devices, or data stored in memory **810**), the device **800** may include components that are configured to encrypt and decrypt the data based on specific algorithms (e.g., DES, 3DES, AES, RSA, etc.). In some embodiments, the processor **812** can execute program code that is stored memory (e.g., in a portion of memory **810**) to carry out certain operations, such as data compression/decompression or data encryption/decryption.

[0074] The device **800** that is depicted in FIG. **8** is one example device that can be configured for generating insurability ratings for a product or service. Such a device includes a first input port coupled to a network communication channel to receive real-time data indicative of cyber attacks that are likely to diminish a value of the product or service. The device also includes a damage assessment computation component that is implemented at least in-part using electronic circuits. The damage assessment computation component is coupled to the first input port to receive the real-time data and compute a real-time damage assessment measure associated with losses to the product or service due to occurrence of one or more cyber-attacks. The damage assessment is computed using at least a likelihood of occurrence of the one or more cyber attacks, a likelihood of success of the one or more cyber attacks, and a measure of severity of damage to the product of service as a result of the occurrence of the one or more cyber attack. The device also includes an insurability rating computation component that is implemented at least in-part using electronic circuits and coupled to the damage assessment computation component. The insurability rating computation component is configured to receive the real-time damage indictor computed by the damage assessment computation component and to determine an insurability rating for the product or service that is usable for determination of an amount of insurance that sufficiently insures against the occurrence of the one or more cyber attacks. The insurability rating is determined at least in-part based on the real-time damage assessment and is changeable in response to changes in the received real-time data.

[0075] The components or modules that are described in connection with the disclosed embodiments can be implemented as hardware, software, or combinations thereof. For example, a hardware implementation can include discrete analog and/or digital circuits that are, for example, integrated as part of a printed circuit board. Alternatively, or additionally, the disclosed components or modules can be implemented as an Application Specific Integrated Circuit (ASIC) and/or as a Field Programmable Gate Array (FPGA) device. Some implementations may additionally or alternatively include a digital signal processor (DSP) that is a specialized microprocessor with an architecture optimized for the operational needs of digital signal processing associated with the disclosed functionalities of this application.

[0076] FIG. **9** illustrates a block diagram of a device **900** that can be implemented as part of the disclosed devices and systems. The device **900** comprises at least one processor **904** and/or controller, at least one memory **902** unit that is in communication with the processor **904**, and at least one communication unit **906** that enables the exchange of data and information, directly or indirectly, through the communication link **908** with other entities, devices, databases and networks. The communication unit **906** may provide wired and/or wireless communication capabilities in accordance with one or more communication protocols, and therefore it may comprise the proper transmitter/receiver, antennas, circuitry and ports, as well as the encoding/decoding capabilities that may be necessary for proper transmission and/or reception of data and other information. The exemplary device **900** of FIG. **9** may be integrated as part of any devices or components to perform any of the disclosed methods.

[0077] Various embodiments described herein are described in the general context of methods or processes, which may be implemented in one embodiment by a computer program product, embodied in a computer-readable medium, including computer-executable instructions, such as program code, executed by computers in networked environments. A computer-readable medium may include removable and non-removable storage devices including, but not limited to, Read Only Memory (ROM), Random Access Memory (RAM), compact discs (CDs), digital versatile discs (DVD), Blu-ray Discs, etc. Therefore, the computer-readable media described in the present application include non-transitory storage media. Generally, program modules may include routines, programs, objects, components, data structures, etc. that perform particular tasks or implement particular abstract data types. Computer-executable instructions, associated data structures, and program modules represent examples of program code for executing steps of the methods disclosed herein. The particular sequence of such executable instructions or associated data structures represents examples of corresponding acts for implementing the functions described in such steps or processes.

[0078] While this document contains many specifics, these should not be construed as limitations on the scope of an invention that is claimed or of what may be claimed, but rather as descriptions of features specific to particular embodiments. Certain features that are described in this document in the context of separate embodiments can also be implemented in combination in a single embodiment. Conversely, various features that are described in the context of a single embodiment can also be implemented in multiple embodiments separately or in any suitable sub-combination. Moreover, although features may be described above as acting in certain combinations and even initially claimed as such, one or more features from a claimed combination can in some cases be excised from the combination, and the claimed combination may be directed to a sub-combination or a variation of a sub-combination. Similarly, while operations are depicted in the drawings in a particular order, this should not be understood as requiring that such operations be performed in the particular order shown or in sequential order, or that all illustrated operations be performed, to achieve desirable results.

What is claimed is:

1. A computer program product, embodied on one or more non-transitory computer media, comprising:

program code for receiving real-time data from a computer network at a processor that is implemented at least in-part by electronic circuitry, the real-time data indicative of cyber attacks that are likely to diminish a value of the product or service;

program code for processing by the processor the real-time data to compute real-time damage assessment associ-

ated with losses to the product or service due to occurrence of one or more cyber-attacks, the damage assessment computed using at least a likelihood of occurrence of the one or more cyber attacks, a likelihood of success of the one or more cyber attacks, and a measure of severity of damage to the product of service as a result of the occurrence of the one or more cyber attacks; and

program code for determining by the processor an insurability rating for the product or service that is usable for determination of an amount of insurance that sufficiently insures against the occurrence of the one or more cyber attacks, wherein the insurability rating is determined at least in-part based on the real-time damage assessment and is changeable in response to changes in the received real-time data.

2. The computer program product of claim **1**, further comprising program code for producing an insurance premium value for the product or service using the insurability rating.

3. The computer program product of claim **1**, wherein the real-time damage assessment is computed on an on-going basis based on changes in the real-time data with a time granularity of 1 micro second or less.

4. The computer program product of claim **1**, wherein the insurability rating is produced at least in-part by:

processing the real-time damage assessment over a pre-determined time interval and determining a statistical value associated with a plurality of insurability rating values over the pre-determined time interval.

5. The computer program product of claim **4**, wherein the statistical value is an average of the plurality of insurability rating values over the pre-determined time interval.

6. The computer program product of claim **4**, wherein the statistical value is a weighted average of the plurality of insurability rating values over the pre-determined time interval, and wherein an insurability rating value that corresponds to a later time instance within the predetermined time interval is assigned a larger weight compared to an insurability rating value that corresponds to an earlier time instance within the predetermined time interval.

7. The computer program product of claim **4**, wherein the pre-determined time interval is one of: one hour, one day, one week or one month.

8. The computer program product of claim **1**, further comprising program code for determining at least one additional insurability rating based on the real-time data, wherein one of the insurability rating or the additional insurability rating corresponds to a short-term insurability rating, and the other of the insurability rating or the additional insurability rating corresponds to a long-term insurability rating.

9. The computer program product of claim **8**, wherein the short-term insurability rating corresponds to a time period ranging from one hour to one day, and wherein the long-term insurability rating corresponds to a time period that is greater than one day and up to one month.

10. The computer program product of claim **1**, wherein the real-time damage assessment is computed using a weighted average technique that assigns a first weight to the likelihood of occurrence of the one or more cyber attacks, a second weight to the likelihood of success of the one or more cyber attacks, and a third weight to the measure of severity of damage to the product of service.

11. The computer program product of claim **1**, wherein each of the likelihood of occurrence of the one or more cyber attacks, the likelihood of success of the one or more cyber attacks, and the measure of severity of damage to the product of service is determined using historical information associated with previously launched cyber attacks against the product or the service.

12. The computer program product of claim **11**, wherein the historical information includes one or more of: a number of previous cyber attacks against the product or service, a rate of success of previous cyber attacks against the product or service, an amount of damage to the service or product caused by a previous cyber attack, or a frequency of occurrence of cyber attacks against other entities that offer products or services that are similar to the product and service.

13. The computer program product of claim **1**, wherein the likelihood of occurrence of the one or more cyber attacks is produced by analyzing data associated with patterns of cyber activity over a plurality of data networks in real-time.

14. The computer program product of claim **13**, wherein the patterns of cyber activity include indications of cyber attacks on organizations with network connectivity.

15. The computer program product of claim **1**, wherein the insurability rating is determined using an inverse proportionality relationship with respect to the real-time damage assessment.

16. The computer program product of claim **1**, wherein the insurability rating is determined based in-part on existing cybersecurity countermeasures that are deployed to protect computers, networks or storage units that participate in storage, production or distribution of the product or service.

17. The computer program product of claim **16**, wherein the insurability rating is modified based on changes in the cybersecurity countermeasures deployed to protect computers, networks or storage units that participate in storage, production or distribution of the product or service.

18. The computer program product of claim **1**, further comprising program code using the computer network for providing one or more of the following to an entity for obtaining or maintaining insurance coverage for the product or service:

information regarding the real-time damage,

information regarding the likelihood of occurrence of the one or more cyber attacks,

information regarding the likelihood of success of the one or more cyber attacks,

information regarding the measure of severity of damage to the product of service as a result of the occurrence of the one or more cyber attacks,

a recommendation for obtaining additional cybersecurity countermeasures, or

a particular cybersecurity countermeasure.

19. A method for producing insurability ratings for a product or service, the method comprising:

receiving, at a processor that is implemented at least in-part by electronic circuitry and coupled to a computer network, real-time data indicative of cyber attacks that are likely to diminish a value of the product or service;

using the processor to process the real-time data to compute a real-time damage assessment associated with losses to the product or service due to occurrence of one or more cyber-attacks, the damage assessment computed using at least a likelihood of the occurrence of the one or more cyber attacks, a likelihood of success of the one or more cyber attacks, and a measure of severity of damage to the product of service as a result of the occurrence of the one or more cyber attacks; and

using the processor to determine an insurability rating for the product or service that is usable for determination of an amount of insurance that sufficiently insures against the occurrence of the one or more cyber attacks, wherein the insurability rating is determined at least in-part based on the real-time damage assessment and is changeable in response to changes in the received real-time data.

20. The method of claim **19**, further comprising using the insurability rating to produce an insurance premium value for the product or service.

21. The method of claim **19**, wherein the real-time damage assessment is computed on an on-going basis based on changes in the real-time data with a time granularity of 1 micro second or less.

22. The method of claim **19**, wherein the insurability rating is produced at least in-part by:

processing the real-time damage assessment over a pre-determined time interval and determining a statistical value associated with a plurality of insurability rating values over the pre-determined time interval.

23. The method of claim **22**, wherein the statistical value is an average of the plurality of insurability rating values over the pre-determined time interval.

24. The method of claim **22**, wherein the statistical value is a weighted average of the plurality of insurability rating values over the pre-determined time interval, and wherein insurability rating values that correspond to later time instances within the predetermined time interval are assigned a larger weight compared to insurability rating values that correspond to earlier time instances within the predetermined time interval.

25. The method of claim **22**, wherein the pre-determined time interval is one of: one hour, one day, one week or one month.

26. The method of claim **19**, further comprising determining at least one additional insurability rating based on the real-time data, wherein one of the insurability rating or the additional insurability rating corresponds to a short-term insurability rating, and the other of the insurability rating or the additional insurability rating corresponds to a long-term insurability rating.

27. The method of claim **26**, wherein the short-term insurability rating corresponds to a time period ranging from one hour to one day, and wherein the long-term insurability rating corresponds to a time period that is greater than one day and up to one month.

28. The method of claim **19**, wherein the real-time damage assessment is computed using a weighted average technique that assigns a first weight to the likelihood of occurrence of the one or more cyber attacks, a second weight to the likelihood of success of the one or more cyber attacks, and a third weight to the measure of severity of damage to the product of service.

29. The method of claim **19**, wherein each of the likelihood of occurrence of the one or more cyber attacks, the likelihood of success of the one or more cyber attacks, and the measure of severity of damage to the product of service is determined using historical information associated with previously launched cyber attacks against the product or the service.

30. The method of claim **29**, wherein the historical information includes one or more of: a number of previous cyber attacks against the product or service, a rate of success of previous cyber attacks against the product or service, an amount of damage to the service or product caused by a previous cyber attack, or a frequency of occurrence of cyber attacks against other entities that offer products or services that are similar to the product and service.

31. The method of claim **19**, wherein the likelihood of occurrence of the one or more cyber attacks is produced by analyzing data associated with patterns of cyber activity over a plurality of data networks in real-time.

32. The method of claim **31**, wherein the patterns of cyber activity are indicative of cyber attacks on other organizations with network connectivity.

33. The method of claim **19**, wherein the insurability rating is determined using an inverse proportionality relationship with respect to the real-time damage assessment.

34. The method of claim **19**, wherein the insurability rating is determined based in-part on existing cybersecurity countermeasures that are deployed to protect computers, networks or storage units that participate in storage, production or distribution of the product or service.

35. The method of claim **34**, wherein the insurability rating is modified based on changes in the cybersecurity countermeasures deployed to protect computers, networks or storage units that participate in storage, production or distribution of the product or service.

36. The method of claim **19**, further comprising providing one or more of the following to an entity that is interested in obtaining or maintaining insurance coverage for the product or service:

information regarding the real-time damage,

information regarding the likelihood of occurrence of the one or more cyber attacks,

information regarding the likelihood of success of the one or more cyber attacks,

information regarding the measure of severity of damage to the product of service as a result of the occurrence of the one or more cyber attacks,

a recommendation for obtaining additional cybersecurity countermeasures, or

a particular cybersecurity countermeasure.

37. A device, comprising:

a processor implemented using electronic circuitry; and

a memory comprising processor executable code, the processor executable code, when executed by the processor, causes the device or the components of the device to:

receive real-time data indicative of cyber attacks that are likely to diminish a value of the product or service;

process the real-time data to compute a real-time damage assessment associated with losses to the product or service due to occurrence of one or more cyber-attacks, the damage assessment computed using at least a likelihood of occurrence of one or more cyber attacks, a likelihood of success of the one or more cyber attacks, and a measure of severity of damage to the product of service as a result of the occurrence of the one or more cyber attacks; and

determine an insurability rating for the product or service that is usable for determination of an amount of insurance that sufficiently insures against the occurrence of the one or more cyber attacks, wherein the insurability rating is determined at least in-part based on the real-time damage assessment and is changeable in response to changes in the received real-time data.

38. A device for generating insurability ratings for a product or service, comprising:

a first input port coupled to a network communication channel to receive real-time data indicative of cyber attacks that are likely to diminish a value of the product or service;

a damage assessment computation component that is implemented at least in-part using electronic circuits, the damage assessment computation component coupled to the first input port to receive the real-time data and compute a real-time damage assessment measure associated with losses to the product or service due to occurrence of one or more cyber-attacks, the damage assessment computed using at least a likelihood of occurrence of the one or more cyber attacks, a likelihood of success of the one or more cyber attacks, and a measure of severity of damage to the product of service as a result of the occurrence of the one or more cyber attack; and

an insurability rating computation component that is implemented at least in-part using electronic circuits and coupled to the damage assessment computation component, the insurability rating computation component to receive the real-time damage indictor computed by the damage assessment computation component and to determine an insurability rating for the product or service that is usable for determination of an amount of insurance that sufficiently insures against the occurrence of the one or more cyber attacks, wherein the insurability rating is determined at least in-part based on the real-time damage assessment and is changeable in response to changes in the received real-time data.

39. A system for determining insurability rating of a service or product, comprising:

a server device coupled to a computer network to receive real-time data indicative of cyber attacks that are likely to diminish a value of the product or service and to produce an insurance premium estimate based at least in-part on the received real-time data;

a client device coupled the computer network to receive the insurance premium estimate produced by the server device, wherein:

the server device uses the real-time data to compute a real-time damage assessment associated with losses to the product or service due to occurrence of one or more cyber-attacks, the damage assessment computed using at least a likelihood of occurrence of the one or more cyber attacks, a likelihood of success of the one or more cyber attacks, and a measure of severity of damage to the product of service as a result of the occurrence of the one or more cyber attacks, and

the sever device determines an insurability rating for the product or service that is usable for determination of an amount of insurance that sufficiently insures against the occurrence of the one or more cyber attacks, the insurability rating determined at least in-part based on the real-time damage assessment and is changeable in response to changes in the received real-time data.

* * * * *